ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2013.0104

ON SECURE FULL DUPLEX COMMUNICATION IN MOBILE AD HOC NETWORK

S. C. Dutta[1], Sudha Singh[2] and D. K. Singh[3]
[1]*Department of Computer Science and Engineering, Birsa Institute of Technology Sindri, India*
E-mail: dutta_subhash@yahoo.com
[2]*Department of Computer Science and Engineering, Bengal college of Engineering and Technology, India*
E-mail: sudha_2k6@yahoo.com
[3]*Department of Electronics and Communication Engineering, National Institute of Technology Patna, India*
E-mail: dksingh_bit@yahoo.com

Abstract
This paper is to establish Ad Hoc network in mobile phones and start fully secured full duplex communication in any situation. This type of communication will be cost effective and it will be fastest way of communication in case of any server failure or server error.

Keywords:
Wireless Ad Hoc Network, Mobile Ad Hoc Network, Bluetooth, Half Duplex Communication, Full Duplex Communication

1. INTRODUCTION

An ad hoc wireless network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range (peer-to-peer communication) or one that is outside their radio range (remote-to-remote communication) using intermediate node(s) to relay or forward the packet from the source (sender) toward the destination (receiver). An ad hoc wireless network is self-organizing and adaptive.

The ad hoc network can be heterogeneous, i.e., the nodes can be of different types (palmtop, laptop, mobile phone...) with different computation, storage and communication capabilities. In mobile computing environments mobile wireless devices that have the capability to detect the presence of existing networks can be used to synchronize data with the user's conventional desktop computers automatically, and download appointment / schedule data. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. These areas could be military battlefield or some flood or earthquake affected areas. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multihop routing. But these networks are more vulnerable to security threats, so secure communication is very much required.

Now a day communication between two mobile phones is not cost effective. For each SMS there is a charge by the service provider and it becomes worthless when we are communicating in shorter distances and if there is any server failure or server error then we cannot communicate, at that point of time proposed work seems to be cost effective and the fastest way of secure communication.

2. LITERATURE REVIEW

Efficient and improved methods of secured data transmission in mobile ad hoc networks (MANETs) are most recent research issues for full applicability of deploying MANETs in wide range of applications.

Of particular interest are systems which may be deployed in an ad hoc manner. These systems cannot make use of pre-existing infrastructure, everything necessary to create a functional systems to be deployed anywhere, at anytime [2]. History of the networking and spectrum aspects of common data link has been discussed by Yang et al. Pa[4].

In a paper by khan et al.[5], an extended DSDV protocol has been used to provide full duplex connectivity between exclusive ad hoc hosts and the hosts of the wired network. The strategy does not take into account the visiting mobile nodes of the infrastructure network, to join the ad hoc network and access the wired network resources. Their proposed framework uses one of the ad hoc hosts known as mobile gateway node to act as a bridge between ad hoc network and the wired network. In a paper by Bechler et al. [9], author proposed and evaluated a security concept based on a distributed certification facility. A network is divided into clusters with one special head node each. These cluster head nodes execute administrative functions and hold shares of a network key used for certification. New node start to participate in the network as guests; they can only become full member with a network signal certificate after their authenticity has been warranted by some other members.

Paper, by Wang et al.[7], presents the design, implementation and evaluation of full duplex attachment system, a cross layer system to solve both hidden terminal problems and exposed terminal problems. In the paper, by Bassily et al.[11], authors studied the role of co-operative relays to provide and improve secure communication rates through decode and forward strategies in a full duplex multiple relay network with an eavesdropper. In the paper, by Wasef and Xuemin[1], authors proposed expedite message authentication protocol for VANETs which replaces the time consuming certificate revocation lists(CRLs) checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed hash message authentication code. In the paper, by Sarker and Mouftah[3], authors studied about mitigating the effect of jamming signals using multipacket transmission and/or multipacket reception capabilities of each node. An optimal transmission scheduling scheme for full duplex relaying and half duplex relaying hybrid is proposed by Yammamoto et al [6]. The scheme is formulated as an optimization problem. Kyung Ah

Shim [12] proposed a conditional privacy preserving authentication scheme, called CAPS, using pseudo-identity based signatures for secure vehicle to infrastructure communications in vehicular ad hoc networks.

Due to raising dependence of people on critical applications and wireless network, high level reliability, security and availability is claimed to assure secure and reliable service operation. Wireless ad hoc networks experience serious security issues even when solutions employ preventive or reactive security mechanisms. In order to support both network operations and security requirements of critical applications, authors in [10] presented a survivable ad hoc and mesh architecture (SAMNAR). They use SAMNAR to design a path selection scheme for WANET routing.

According to the Tian Lan et al.[8], full key connectivity cannot be achieved by key pre-distribution due to physical limitations and scalability requirements. They developed an analytical framework for the on demand key-establishment approach, considering mainly revealing, erasure and modification attacks. But for most urgent secure communication, this is not secure because unauthorized user are getting access to those keys specially in MANETs.

Secure mobile communications in wireless ad hoc networks require setting end-to-end secret keys for communicating nodes. In this paper, we established secure communication between mobile nodes in case of almost all types of attacks including revealing, erasure and modification (REM) attacks. Literature analysis shows that this work has not been done before for wireless ad hoc network. Resources used in the proposed system are, (a) the computer language used to develop this application, J2ME (Java 2 Micro Edition), (b) JSR 82 API (application programming interface), (c) L2CAP (Logical link control and adaption protocol), the protocol used for communication.

3. SYSTEM MODEL AND DESCRIPTION

This system has basically two parts one is server part and other is the client part server part is responsible for connecting with client machine and receiving messages while client part is responsible for sending connection request to the server machine and sending messages. This system can be divided into three categories as shown in Fig.1.

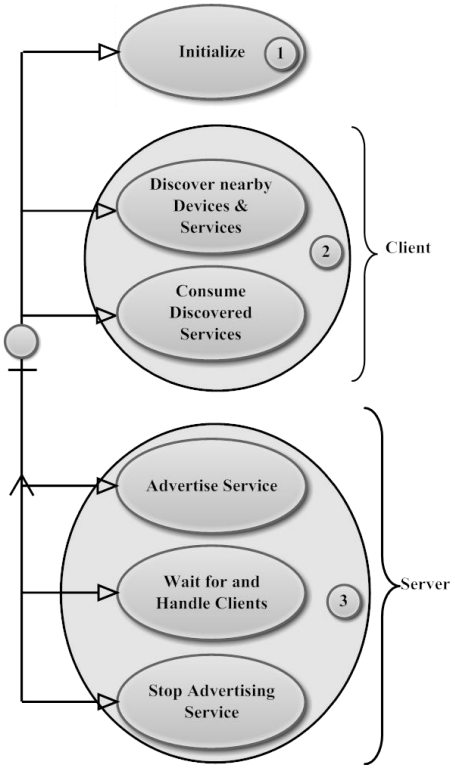

Fig.1. Categories of proposed system

First part is initialization second part is client part and the third part is server part. In Initialization, any Bluetooth-enabled application, server or client, must first initialize the Bluetooth stack.

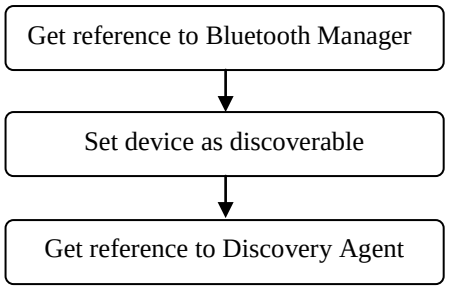

Fig.2. Initialization part of proposed system

First the application retrieves a reference to the Bluetooth Manager from the LocalDevice. Client applications retrieve a reference to the DiscoveryAgent, which provides all the discovery-related services. Server applications make the device discoverable. In the following code snippet, the initialization method btInit() performs both client and server initialization:

```
...
private LocalDevice localDevice; // local Bluetooth
                                                Manager
private DiscoveryAgent discoveryAgent; // discovery
                                                agent
...
/**
 * Initialize
 */
public void btInit() throws BluetoothStateException {
    localDevice = null;
    discoveryAgent = null;
    // Retrieve the local device to get to the Bluetooth
          Manager
    localDevice = LocalDevice.getLocalDevice();
    // Servers set the discoverable mode to GIAC
    localDevice.setDiscoverable(DiscoveryAgent.GIAC);
    // Clients retrieve the discovery agent
    discoveryAgent = localDevice.getDiscoveryAgent();
}
...
```

In server part, a server makes services available to clients. It registers them in the Service Discovery Database (SDDB), in effect advertising them. It then waits for incoming connections, accepts them as they come in, and serves the clients that make them. Finally, when the service is no longer needed the application removes it from the SDDB.

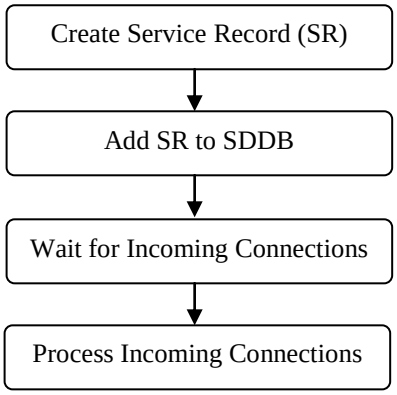

Fig.3. Server part of proposed system

In creating a service record, the bluetooth implementation automatically creates a service record when application creates a connection notifier, either a StreamConnectionNotifier or an L2CAPConnectionNotifier.

In registering the service and waiting for incoming connections, the server is ready to register the service and wait for clients.

```
Invoking the notifier's acceptAndOpen() method
...
// Insert service record into SDDB and wait for an
incoming client
StreamConnection conn =
streamConnectionNotifier.acceptAndOpen();
...
```

Updating the Service Record – There are occasions when the attributes for a registered service must be changed. We can update records in the SDDB using the local Bluetooth manager. As the next snippet shows, we retrieve the record from the SDDB by calling LocalDevice.getRecord(), add or change attributes of interest by calling ServiceRecord.setAttributeValue(), and write the service record back to the SDDB with a call to LocalDevice.updateRecord():

```
...
try {
    // Retrieve service record and set/update optional
attributes,
    // for example, ServiceAvailability, indicating service
is available
    sr =localDevice.getRecord(streamConnectionNotifier);
   sr.setAttributeValue(SDP_SERVICEAVAILABILITY,
        new DataElement(DataElement.U_INT_1, 0xFF));
    localDevice.updateRecord(sr);
} catch (IOException ioe) {
    // Catch exception, display error
}
...
```

In client part, a client consumes remote services. It first discovers any nearby devices, then for each discovered device it searches for services of interest. Algorithm for discovering nearby devices and services is given below:

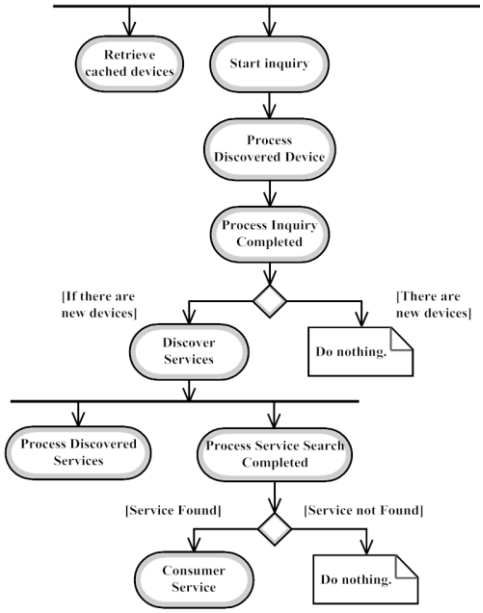

Fig.4. Client part of proposed system

To receive discovery notifications from the DiscoveryAgent the client application must implement the DiscoveryListener interface and its four discovery callbacks deviceDiscovered(), inquiryCompleted(), servicesDiscovered(), and serviceSearchCompleted().

Connecting to a Service – Once a service of interest has been found, the client application can connect to it. As you learned earlier, the client can retrieve the service's connection URL from its service record.

Securing a Bluetooth Connection – A secure Bluetooth connection is one that is authenticated, and optionally authorized, and encrypted. A Bluetooth connection can be secured when it's established, or later.

To make a Bluetooth connections secure when you establish it you must ensure that the javax.microedition.io.Connector connection URL string has the appropriate security parameters:

```
btspp://hostname:[CNUUID];authenticate = true;
authorize = true; encrypt = true
```

where,

- authenticate verifies the identity of a connecting device.
- authorize verifies its access to a given service. Authorize is not allowed on client URL connection strings.
- encrypt specifies that the connection must be encrypted.

Accepting the messages send by the client-:

The following code is responsible for the messages send by client to server:

```
for (;;) {
    StreamConnection conn =notifier.acceptAndOpen();
    OutputStream output = conn.openOutputStream();
    InputStream input = conn.openInputStream
    byte [ ] data = new byte[10];
    int length =0;
    while ((length = input.read(data)) != -1) {
    form1.append(new String(data, 0, length));
    output.write(data, 0, length);
    output.flush();
}
```

Snapshots of the proposed system are given below:

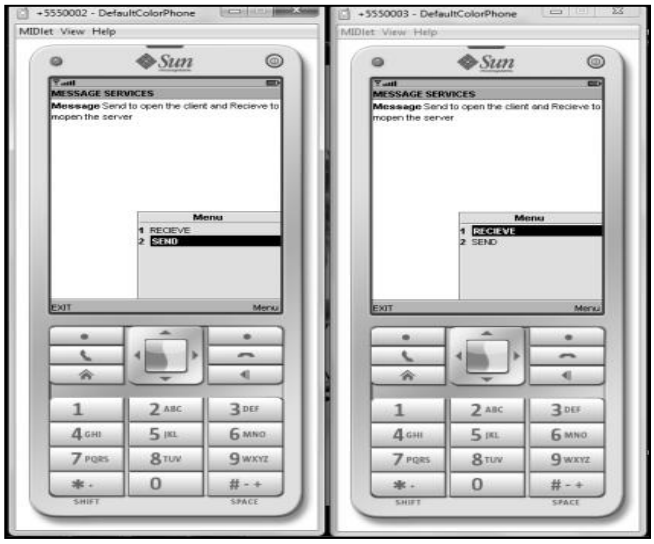

Fig.5. Snapshot 1

Fig.6. Snapshot 2

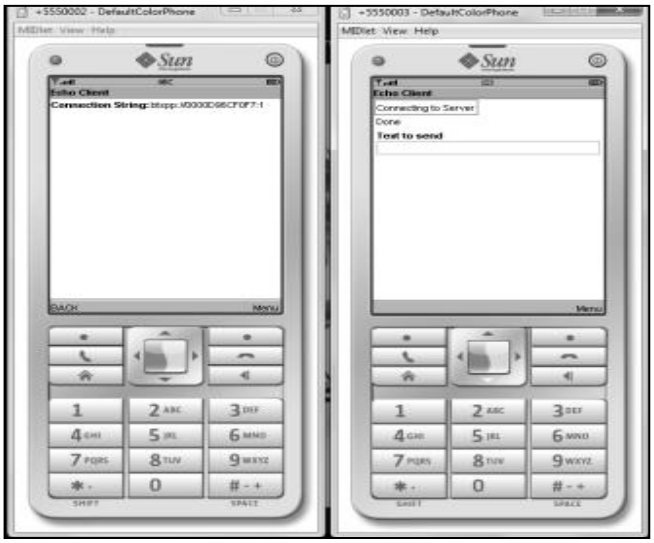

Fig.7. Snapshot 3

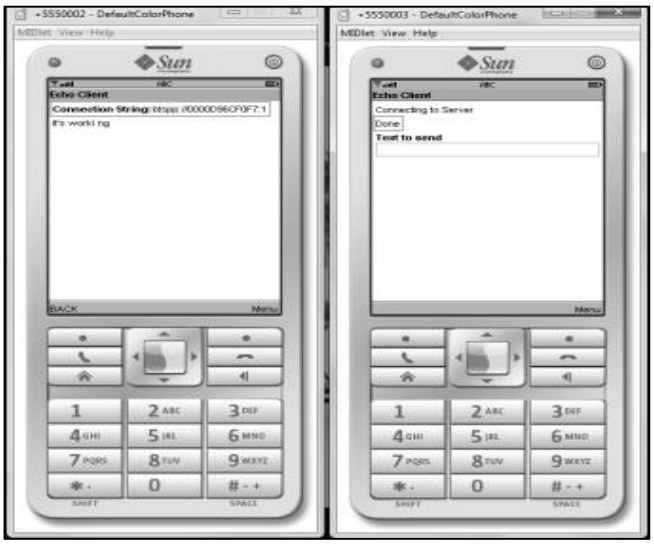

Fig.8. Snapshot 4

Fig.9. Snapshot 5

Fig.10. Snapshot 6

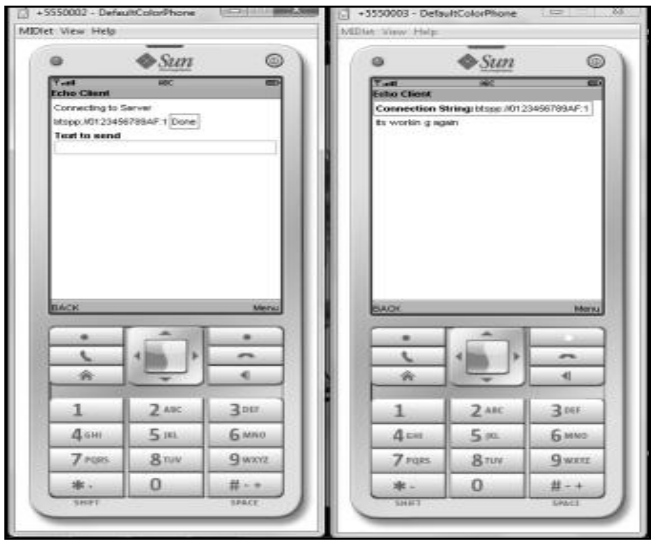

Fig.11. Snapshot 7

Features of the proposed system are,

- This application helps in cost effective communication because the technology used to develop this project is java based which is compatible without any extra cost and do not need a specific platform.
- Since two mobiles connected once only via Bluetooth and then there is message sending, so the communication through this is relatively faster than other traditional ways of communication.
- In this technology connection strings are developed randomly based on mobile phone hardware which is later used for connecting two mobiles. That is why it is also secured and reliable way of communication.
- Since the graphical user interface of this application is simple, so it is simple to use for the user of this application.
- Since the application having very relevant size (14 kb) it uses very little mobile resources and produces a good way of communication.

Security:

The following is a list of security requirements that indicate how the system shall protect itself and its sensitive data and communications from accidental, malicious, or unauthorized access, use, modification, or destruction.

- The system shall not allow Bluetooth addresses of unauthorized Bluetooth devices to be stored into the system's repository.
- The system shall not permit unauthorized Bluetooth devices to access or participate in any activity started by the server (mobile) user.
- The system shall not allow confidential data stored in the system's database to be accessed, whether directly or indirectly, by client (mobile) users.
- The system shall force the laptop user to confirm any data deletion to prevent any accidental erasure of sensitive data.

4. CONCLUSION AND FUTURE WORK

A full duplex mode secure communication has been established between mobiles using Bluetooth. So that users can share the text messages among themselves. It is cost effective and faster than other conventional method of communication. But the major difficulty with this is that it is successful in short range within 20m only. Future work may include increasing range and to provide a more option like sharing photos with his friend who is connected through user so that he can send a photo using this application not only text. We are also working on access the memory card or a particular file of one mobile to other mobile using Bluetooth connectivity. In further modification we are also trying to control PC through mobile phones.

REFERENCES

[1] Wasef and Xuemin Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks", *IEEE Transactions on Mobile Computing*, Vol. 12, No.1, pp. 78 - 89, 2013.

[2] F. Progri, W. R. Michalson and M. C. Bromberg, "Accurate synchronization using full duplex DSSS channel", *Proceedings of IEEE Conference on Position Location and Navigation Symposium*, pp. 220 - 226, 2004.

[3] J. H. Sarker and H. T. Mouftah, "Mitigating the effect of jamming signals in wireless ad hoc and sensor networks", *IET communications*, Vol. 6, No. 3, pp. 311- 317, 2012.

[4] J. Yang, John Boyd, David Laney and Jennifer Schlenzig, "Next generation half duplex common data link", *Proceedings of IEEE International Conference on Military Communications*, pp. 1 - 7, 2007.

[5] K. U. R. Khan, R. U. Zaman and A. V. Reddy "A bidirectional connectivity framework for mobile adhoc network and the internet", *Proceedings of 1st IFIP wireless days*, pp. 1- 5, 2008.

[6] K. Yamamoto, K. Haneda, H. Murata and S. Yoshida, "Optimal transmission scheduling for a hybrid of full and half duplex relaying", *Letters in IEEE communication*, Vol. 15, No. 3, pp. 305 - 307, 2011.

[7] Lu Wang, Kaishun Wu, Pengfei chang and Mounir Hamdi, "FAST: Realizing what your neighbours are doing", *Proceedings of IEEE International Conference on Communications*, pp. 544 - 548, 2012.

[8] Lan Tian, R Lee and Chiang Mung, "Multipath key establishment against REM attacks in wireless ad hoc networks", *Proceedings of 28th IEEE Conference on Global Telecommunications*, pp. 6255 - 6262, 2009.

[9] M. Bechler, H. Hof, D. Kraft, F. Pahlke and L. Wolf, "A cluster based security architecture for ad hoc networks", *23rd Annual Joint Conference of the IEEE Computer and Telecommunication Societies*, Vol. 4, pp. 2393 - 2403, 2004.

[10] M. Nogueira, H. Silva, A. Santos and G. Pujolle, "A security management architecture for supporting routing services on WANETs", *IEEE Transactions on Network and Service Management*, Vol. 9, No. 2, pp. 156 - 168, 2012.

[11] R. Bassily and S. Ulukus, "Secure communication in multiple relay through decode and forward strategies", *Journal of Communications and Networks*, Vol. 14, No. 4, pp. 352 - 363, 2012.

[12] Shim Kyung-Ah, "Cal CAPS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks", *IEEE Transactions on Vehicular Technology*, Vol. 61, No. 4, pp. 1874 - 1883, 2012.